


**Selection 1**, p. 1 – The following amendment is to reinsert dropped matter which had been included without objection since Amendment C.

**Background -- Field of Invention**



This invention relates to creating and verifying between computers and on computer networks electronic signatures for electronic data, including electronic documents, filings and transaction records.

**Selection 2**, p. 3. The third sentence was deleted in accordance with the objection of the Examiner.

Private keys are susceptible to theft from the computers or devices where they are stored, and when stolen, can be used to commit fraud with virtually no detection until the certificate of the user is revoked by the certification authority with respect to that particular corresponding public and private key pair. Private keys can also be compromised by sharing the passwords used to access them. ~~It is often inconvenient to install the keys and certificates on individual desktop or laptop machines, or to replace them in the event of suspected compromise or upon the certificate's repudiation.~~

**Selection 3**, p. 4. The first two changes had been amended since Amendment C, but had been inadvertently omitted in the Second Substitute Specification; the third, which is a deletion, was matter objected to by the examiner; the last addition in the group was a phrase that had been amended without objection since Amendment B, but was inadvertently omitted from the Second Substitute Specification.

## Objects and Advantages

Accordingly, several objects and advantages of the invention are to provide a new type of electronic signature that does not depend upon the extensive certification authority infrastructure of digital signatures on multiple client machines based on asymmetric encryption or the hardware and software investment of dynamic signatures; further that it uses only a signature key ~~of~~ at a server computer rather than many signature keys of many client computers, further that it can automatically incorporate authentication information about the signer and generate and affix a date and time parameter taken from the server's clock as further evidence of identity authentication at the time of the signature; ~~further that it protects a single key from vulnerabilities through repeated use;~~ signature and verification; further that it eliminates the need for development of a discipline that does not yet exist, namely, the forensic science of electronic handwriting analysis; and that further allows for the use by incorporation of many types of

**Selection 4**, p. 5. These changes had been made without objection, since Amendment C and were inadvertently omitted from the most previous version.

## Summary

In accordance with the present invention, an electronic signature program is described for the creation, monitoring, and verification of an electronic signature generated by the interaction between two computers, one a client and the other a server, for the signing of electronic data, such as documents, filings or transaction records without the need for an expensive and massive infrastructure of certification authorities and the complexities of installing and using digital certificates, ~~without generating conflicts between applicable legal regimes in an international or multi-jurisdictional setting over regulation of the export of encryption software- including cross-~~ certifications, and/or without requiring hardware tablets and associated computer software. This system further is able to incorporate other existing technologies of prior art designed to authenticate users to a server computer and ones not yet available or existing.

**Selection 5**, p. 7. Though not new matter, the amendment provides permissible clarification in accordance with the Examiner's comments and guidance in 2000, as discussed more particularly in the Remarks section.

Creation of the signature is depicted in figure 3. In the preferred embodiment, the server has captured the unique network element parameter of a signer, and where available, a credit card authorization number from a card processor. Where authentication on the basis of stored identity criteria, such as a digital certificate, username and password, or biometrics is involved, alphanumeric elements, appropriate symbols or abbreviations can be used to represent these. Other user identifier elements are known to those skilled in the art and may include a legacy application that has developed a user identifier system. Information from the user elements (no. 18) are combined with the date-time parameters of the server's system clock (no. 19) to create a signature transaction record, optionally with a Globally Unique Identifier (GUID) derived from the blend of the components through message digesting. (no. 20) Because time continuously progresses, each signature transaction that occurs sequentially at the signature server may be uniquely identifiable through the date and time of its creation. A unique network location, expressed as an IP address adds another element of uniqueness where two signature transaction records are created so closely in time as to have identical dates and time of creation. Since it is almost impossible for them to have originated simultaneously from the same network location, a unique network element parameter enables distinguishing between them. Adding identification of the user to the signature transaction, as through a username or a credit card authentication, binds the unique signature 20) transaction record to the user's identity. This combination also permits the server's date and time of record creation to be incorporated under the signature. A hash of the concatenated field values of the unique signature transaction record can serve as a GUID, because each hash of a unique set of values is itself unique. Such a GUID simply can be added as another field of its corresponding signature transaction record as a convenient shorthand unique identifier that can be used to locate, refer to, or identify it.

**Selection 6**, p. 7. The sentence beginning "Encapsulation consists of ..." was objected to by the examiner and was deleted. The text immediately following that deleted sentence had been inadvertently omitted from the Second Substitute Specification and had been in the specification without objection since Amendment C. The other changes are for clarity only

Figure 4 demonstrates how the GUID is used to encapsulate how the digital signature of the server computer digitally wraps the data. An active X (com) object or other applications programming interface (API)(no. 23) at the Internet server communicates with the signature program of the Internet server to hash and sign the information (no. 22) to be contained under the signature (no. 21) ~~with the server's private key~~. ~~Encapsulation consists of symmetrically encrypting a detached digital signature's value, using the GUID or component of it as the password or seed (no. 24).~~ 21), including the unique signature transaction record fields, which may be represented by the GUID, with a private key located at the server. Once the signature is thus ~~digitally wrapped, it generated~~, it also constitutes signature transaction meta-data that is stored at the server and can be included in an automatically generated email message (no. 25). ~~It 25) which~~ is sent to the user at the email address that the user self-reported to the Internet server initially.

**Selection 7**, bottom p. 7, top p.8. This section deletes material objected to by the Examiner.

~~To verify a signed document, it is resubmitted to the server, where the symmetrically encrypted version of the digital signature is decrypted by recreating the symmetric key from the signature transaction record components, and applying it, and then normal verification on the basis of the server's public key is invoked.~~

**Selection 8**, p. 8. The following portion is simply being moved without modification to the last page of the Second Substitute Specification for clarity and so it is shown as a deletion here and later as an addition to the Specification.

~~The encrypted digital signature ensures that the information included as the basis for the symmetric key, including signature transaction record particulars, date and time values, and electronic signature cannot be altered after the fact without such change being detectable through software upon verification.~~

**Selection 9**, p. 8. The deleted material in the next section was objected to by the Examiner and the earlier version has been reinstated with the minor additional phraseology for clarity.

~~The preferred embodiment also enables signer-supplied form submission data to be inserted into appropriate locations in a transaction template to be signed as part of a completed document.~~ digitally signed wrapper also permits signer-supplied submission information to be inserted into a document to be included under the server signature which is stored at the server as part of a transaction template, and which may include standard terms applicable to the class of transactions. ~~This enables standardized contracts and clauses to be included in legally binding contracts.~~ The template may simply be a blank (structure only) document, to be filled in completely by the user, or it also may include "boilerplate", meaning standardized language that is intended to remain in the document. Boilerplate is commonly associated with legal, financial, real estate and mortgage phrases and provisions that are intended as inalterable in the document finalization and signature process. For example, it can include standard terms for purchase orders. For example, it can include notices and averments to governmental regulatory bodies. For example, it can include electronic credit card charge slips. By putting the boilerplate terms and conditions at the server and incorporating them as a template for signer data to complete and to be included under the signature, that cannot be modified by a signer, unauthorized pre-signature modifications are prevented. For example, in an extreme example, the template located on the server consists completely or almost entirely of boilerplate language that the signer is expected to accept and sign or reject without adding, modifying or inserting any information specific to the signer or transaction. For example, the transaction template may be used to generate an envelope

for the transmission and routing of one or more documents or files that are embedded into the envelope. Any of the documents and files with a potential to be embedded in or attached to an envelope can also be signed using this invention.

invention. In each case, the template is signed by the server as part of the data that is included under the signature affixed on behalf of the signer along with the previously described unique signature transaction information, which may be represented in shorthand fashion by its corresponding GUID.

**Selection 9**, bottom p. 8, top p. 9. The deleted material below was objected to by the Examiner and added material has been reinstated from the earlier version for clarity.

Return of signature transaction this information to the individual who signed the information in an email message serves as a receipt and proof from the server of a valid signature transaction. Such a proof of transaction can be asymmetrically signed by the server, providing inalterable proof successful signature verification as of a is a receipt that is proof of the transaction, the electronic signature, and the transaction content.

particular time. If the email address is non-existent, intermediate mail server computers usually alert the server via a failed email message that the message was undeliverable. Such a message also serves to warn the server computer that a fraudulent transaction may be in progress.

**Selection 10**, p. 10-11. The first two minor changes were added without objection by Amendment C. The Examiner objected in the OA to the last several sentences of the section which have been deleted.

## Conclusions, Ramifications, and Scope

Accordingly, it can be seen that the above system allows client computer users to sign electronic documents, filings and transaction records submitted to a server computer as though with pen and ink on paper, without any additional hardware or software apart from an Internet web browser. The signature program reduces the need for a massive infrastructure investment of certification authorities by relying solely upon the ~~a digital certificate of~~ at the server computer, without any similar requirement that the signing party obtain a separate digital certificate, unless optionally required for receipt signing purposes. The method is able to make use of other current and future technologies for computer user authentication systems, and is suited for the Internet and other computer networks. ~~The use of a second encryption layer has a further advantage of protecting the private key. Without the symmetric digital wrapper that changed with each signer transaction, an attacker might be~~ networks. ~~able to deduce the private key attributes from an examination of a myriad of signatures and hash values. The symmetrically encrypted signature value also can serve to protect the underlying asymmetric signature at a future time when a factoring attack on asymmetric signatures by significantly more powerful computers may become computationally feasible. The symmetric encryption of the returned asymmetric signature value serves to shield the asymmetric private key from a factoring attack as the symmetric enciphering wrapper cloaks the asymmetric signature value, hiding it from the attacker.~~

**Selection 11**, p. 11-12. In the next section, the deleted material was objected to by the Examiner; the added material is being reinstated from a prior version. The next to the last sentence is reinstated because it was accidentally omitted in the most previous version and was added without objection to Amendments C and D respectively. The very last sentence was simply moved from another page (p.7) to this one for clarity of expression.

Although the description above contains much specificity, this should not be construed as limiting the scope of the invention but as merely providing illustrations of some of the presently preferred embodiments of this invention. Various other embodiments and ramifications are possible within its scope. For example, other unique system information of the server can be used in addition to the system clock to generate a unique record and its GUID, which may also be encrypted.

Modification within the spirit of the invention will also be apparent to those skilled in the art. ~~For example, other unique system information of the server can be used in addition to the system clock to generate a signature transaction record, all or parts of which may also be encrypted. For example, copies of a single asymmetric key may be distributed among several different servers, or a single server may have a number of different asymmetric keys for use by each of various assigned individuals, entities or groups. For example, signers may be authenticated by trusted third party assertions. For example, a message digest generated during signature may be encrypted only using a symmetric key, rather than an asymmetric key, bypassing a second encryption step. Alternatively, the symmetric encryption of the message digest may precede the asymmetric encryption, allowing the asymmetric encryption to act as a digital wrapper for the symmetric encryption. For example, electronic processes may sign as client users on behalf of individuals or entities. For example, enveloped or enveloping digital signatures may be generated using this invention in addition to detached digital signatures.~~

in another embodiment, the GUID may be used as the password or seed for a symmetric encryption cipher known to one skilled in the art such as RC4 to generate a unique encryption key. Application of this key to the document to be signed symmetrically encrypts the document. This encrypted version of the document is unique and constitutes the signature of the document. To verify the document, either the encrypted version is decrypted using the unique key, or the presented version for verification is re-encrypted using the unique key. If the presented document



is genuine, the two end products will be identical. As the GUID contains also information about the identity of the signer, an electronic signature is created. As an intermediate step in the signature process, the document may optionally be hashed or digested prior to encryption with the symmetric cipher. This symmetric encryption cipher embodiment differs from the preferred embodiment, in that in the latter, a message digesting function or asymmetric key pair is used for the signature and verification functions[[.]], while in the former, in a second stage, symmetric encryption can be used to encrypt the intermediate digest or private key signature arrived at using the preferred embodiment. The encrypted digital signature ensures that the information included as the basis for the symmetric key, including signature transaction record particulars, date and time values, and electronic signature cannot be altered after the fact without such change being detectable through software upon verification.

Please see the Remarks section for further analysis and discussion.